

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with following Twitter profiles:  
@OfficialJigLord; @TacticalIntern; @jighelperDM;  
@TryFaceOn; @BawbyJordan; @SKRGANG; and  
@Potatohead1521 stored at premises owned, maintained,  
controlled, or operated by Twitter. See Attachment A.

Case No. 19-836M(KT)

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Information associated with the following Twitter profiles: @OfficialJigLord; @TacticalIntern; @jighelperDM; @TryFaceOn; @BawbyJordan; @SKRGANG; and @Potatohead1521 stored at premises owned, maintained, controlled, or operated by Twitter. See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 1343; 18 U.S.C. § 1029(a)(2); and 18 U.S.C. § 1029(a)(3).

The application is based on these facts: See attached affidavit.

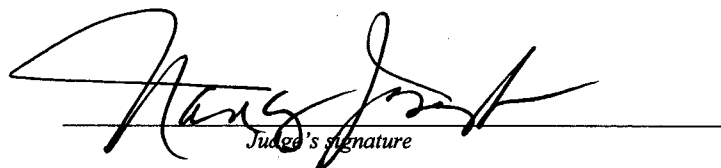
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Special Agent Zachary Hoalcraft, United States Secret Service  
Printed Name and Title

Sworn to before me and signed in my presence:

Date: February 26, 2019

  
Judge's signature

City and State: Milwaukee, Wisconsin

Nancy Joseph, U.S. Magistrate Judge  
Printed Name and Title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Zachary Hoalcraft, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Twitter account that is stored at premises owned, maintained, controlled, or operated by Twitter, a social-networking company headquartered in San Francisco, CA. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Twitter to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Twitter account.

2. I am a Special Agent with the United States Secret Service and have been employed so since 2017. I am currently assigned to the U.S. Secret Service Milwaukee Financial Crimes Task Force (MFCTF). My duties include investigations into financial crimes, such as identity theft, check fraud, credit card fraud, bank fraud, wire fraud, currency-counterfeiting offenses, and money laundering. As a Task Force Agent, I have conducted investigations into wire fraud, money laundering, and other complex financial crimes. In the course of those investigations, I have used various investigative techniques, including undercover

operations, reviewing physical and electronic evidence, and obtaining and reviewing financial records. In the course of these investigations, I have also become familiar with techniques that criminals use to conceal the nature, source, location, and ownership of proceeds of crime and to avoid detection by law enforcement of their underlying acts.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1029(a)(2) (trafficking in unauthorized access devices), and 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized access devices)<sup>1</sup> have been committed by Robert Gordon, a/k/a @OfficialJigLord and his associates. There is also probable cause to search the information described in Attachment A for evidence of these crimes as described in Attachment B.

---

<sup>1</sup> For purposes of 18 U.S.C. § 1029, “the term ‘access device’ means any . . . code, account number, electronic serial number, mobile identification number, personal identification number, . . . or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value[.]” 18 U.S.C. § 1029(e)(1). “[T]he term ‘unauthorized access device’ means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.” 18 U.S.C. § 1029(e)(3).

### **PROBABLE CAUSE**

5. Kohl's Department Stores, Inc. ("Kohl's"), headquartered in the State and Eastern District of Wisconsin, is a retail chain that purchases and sells items in interstate and foreign commerce.

6. Kohl's operates a customer loyalty rewards program called "Yes2You Rewards." Kohl's customers can sign up to be rewards program members and earn reward points. These points are periodically converted to "Kohl's Cash," based on purchases made at or through Kohl's. A certificate with the amount of "Kohl's Cash," along with a bar code number, PIN number, and expiration date, is periodically sent to the member. The member can then redeem the rewards "Kohl's Cash" for additional purchases at or through Kohl's. If there is a balance left after application of rewards "Kohl's Cash" to a purchase, the purchaser can apply another payment form, such as a credit card. Customers may view and print their Kohl's Cash and rewards items by setting up an account through Kohl's website, Kohls.com, which includes creating their own unique username and password. Customers may also make online purchases through their account on Kohls.com.

7. In addition to receiving "Kohl's Cash" rewards in the form of paper certificates, customers can install the Kohl's Mobile Wallet application on their electronic devices. With the Kohl's Mobile Wallet, customers are able to view, use, or upload their "Kohl's Cash" rewards.

8. On July 19, 2018, a Senior Representative for Social Media at Kohl's discovered a Twitter account, @OfficialJigLord, that had postings that referenced

the sale of Kohl's Cash by the account holder. On August 13, 2018, a Kohl's customer representative received a direct message on Kohl's corporate Facebook account from a concerned citizen. The message states "Hi, this account @OfficialJigLord steal customers info and sells their Kohl's Cash on twitter. Just checkout his tweets and you will see for yourself. LMK if there is anything I can do to help you catch him. Something needs to be done."

9. The investigation thus far shows that @OfficialJigLord has been actively engaged in the activity described herein from at least July 2018, through the present. In summary, the investigation reveals that @OfficialJigLord is involved in a scheme that unlawfully accesses Kohl's customers' accounts and steals Kohl's Cash from those accounts. @OfficialJigLord then advertises and sells the stolen Kohl's Cash through his Twitter account, and uses some himself.

10. Information obtained from @OfficialJigLord's public Twitter feed, as observed by Kohl's staff and law enforcement, has been helpful in the investigation. This information included postings by @OfficialJigLord's of photographs of receipts from Kohl's, photos of items purchased at Kohl's with comments on the photos, notes regarding Kohl's Cash, discussions about Kohl's Cash, and other social media profiles he uses.

11. Among other things, Kohl's observed that @OfficialJigLord claims in his Twitter feed to use a "bot" to access Kohl's customer accounts via Kohl's public retail website. It also appears that @OfficialJigLord obtains customer rewards from other companies as well, based on comments to his Twitter account. The term "bot"

generally refers to a program that runs autonomously and can perform repetitive and remotely controlled tasks.

12. The use of a “bot” was discussed by @OfficialJigLord in his Twitter feed. For example, on August 20, 2018, @OfficialJigLord posted a photograph on his Twitter account that appeared to be a screenshot of a computer running a bot under the caption “Getting more AE. Don’t you all worry too much.” The words “BOT STATUS: SUCCESS” can be seen in the upper left of the screenshot, and a series of characters, including words “‘expiration date’: ‘2018-09-16’, ‘issueDate’: ‘20 [screen cutoff]’” can be seen in the background behind a banner reading “Breaking News.” In another posting, @OfficialJigLord states “Will have about 20 more batches of CFA I think this evening. Bot still running. Also should have some more QDoba, ULTA, and Rasing Canes.”

13. On August 19, 2018, @OfficialJigLord posted “Ok does everyone remember how the new period Kohl’s batch goes? New Period begins tomorrow August 20th. Balance activates at midnight CST tonite. I will honor 8 hour warranty due to store not opening until 8 AM. If you use it online and it gets cancelled, no refunds.”

14. In another posting, @OfficialJigLord posts “Warranty for Kohl’s Cash new period (EST, CST, and MST) is up. For my PST folks, you have exactly 2 hours remaining. Don’t forget to post and tag me in your success!”

15. On August 26, 2018, @OfficialJigLord posted: "Two \$400 batches of Kohl's available. Price is \$200 each. In store use only. Use today. Zelle or CashApp only. DM if interested."

16. On another date, @OfficialJigLord posted a list of eight readable Kohl's Cash rewards (there were two rewards that were only partially shown), each noting the number, PIN, value, "Valid till" date, "startdate" and "enddate." The posting came under the caption "#IYKYK" (which appears to mean "if you know, you know" as in "you understand what is going on"). Kohl's checked their records and found that the 8 readable rewards Cash coupons listed in the posting were earned by seven different Kohl's rewards members with initials M.R., B.F., R.C., G.W., S.B., R.L., C.K. The rewards were redeemed by four different customers with initials C.R., M.P., J.B., A.L, who presumably purchased the rewards from @OfficialJigLord.

17. On September 2, 2018, @OfficialJigLord posted: "\$165 Kohl's batch available for instore use. Read FAQ if you're new. If you know how it works, DM me to purchase." This post is referring to a Twitter posting called Jiglord University. This posting contains four tabs with titles of Kohl's, AMC, AmericanEagle, and Chipotle. Under the Kohl's tab, there is an explanation regarding purchasing and redeeming Kohl's Cash obtained from @OfficialJigLord. @OfficialJigLord explains that Kohl's Cash can be used in store and online, suggests how to use the Kohl's Cash, and explains how @OfficialJigLord has a warranty on batches of Kohl's Cash sold by @OfficialJigLord. There is an explanation that @OfficialJigLord sells Kohl's

Cash at 50% of face value and that payments to @OfficialJigLord are accepted through the use of Zelle and CashApp, which are applications that allow for digital transfer of funds between parties.

18. On November 7, 2018, @OfficialJigLord posted: "Not a lot of stock today. Program kept crashing out on me last night. Woke up this morning and it had forced flossed caus of a stupid ass update. Today I have about \$2000 in Kohls and about \$1000 in Starbucks. Will open DMs in about 15 min."

19. @OfficialJigLord encourages his "customers" to "tag" him in postings announcing their success in using Kohl's Cash purchased from @OfficialJigLord. Several "customers" did so, by among other things, posting photographs of their items or receipts from Kohl's following a successful purchase. For example, on August 14, 2018, "Danny" tagged @OfficialJigLord in a posting that included a photograph of a box containing cooking wear and a Nest thermostat device under the caption "@OfficialJigLord . . . No airpods but did some good ol' adulating and bought some nice household items." For another example, on September 8, 2018, "Richard" posted a photograph of a Kohl's receipt showing numerous Kohl's Cash amounts credited to a purchase of at least \$298.60" with the caption "@OfficialJigLord thanks bro. lots of candles." And another date, "Camour" posted a screenshot showing a successful order of Apple AirPods and a caption "@OfficialJigLord thanks to jiglord I was able to cop 2 Apple airpods. #OfficialJigLord #deal #steals #jig #copped #winner."



20. On another date, @OfficialJigLord tweeted: "Before I sell something I haven't sold, you guys know I have to test it first that way I can give you all no fail instructions. More to follow on Shell discounts." This post appears to refer to @OfficialJigLord testing fraudulently obtained rewards codes for different retailers (including Shell gas stations) prior to advertising them for sale on Twitter.

21. According to Kohl's, and as explained further herein, Kohl's reviewed its records and open-source information associated with @OfficialJigLord's Twitter feed and concluded that @OfficialJigLord is most likely Robert A. Gordon ("Gordon") of Weston, Wisconsin, who has registered an account with Kohl's. Kohl's was able to identify an IP address, 66.188.227.231, associated with Gordon's account information. By comparing that IP address against records of logins to Kohl's website, Kohl's found that the IP address appeared to be connected to identity theft activity. For instance, Kohl's records showed that from around July 23, 2018 through October 3, 2018, several thousand login attempts to Kohl's webstore were made from that IP address. The login attempts used different, unique usernames and passwords to try to access the website. The usernames were email addresses. A small percentage of the login attempts were successful and Kohl's Cash certificates and their corresponding information (bar number, PIN number, etc.) was exfiltrated from the user's account. This behavior indicates that a program running from a computer at that IP address had a database of email addresses and passwords, possibly stolen from another source such as a business or email provider, and was bombarding Kohl's website with these credentials to steal any Kohl's Cash from

accounts that had the same username (email address) and password for their Kohls' account that was in the larger database. Such behavior could be expedited by "bots" executing the repetitive function and relaying stolen Kohl's Cash to the "bot" operator. Kohl's IT staff concluded that the activity was a computer bot accessing the Kohls.com website from the IP address of 66.188.227.231 in part because the time associated with the access attempts was too short to be accomplished by a human in the time period.

22. In response to a subpoena issued on December 4, 2018, Charter Communication identified that IP address 66.188.227.231 is assigned to customer Diana Gordon at 5815 Stella Ave., Weston, WI 54476. Diana Gordon has been identified as Robert Gordon's wife. Further investigation revealed that Robert A. Gordon is a Staff Sergeant and active reserve member of the U.S. Army assigned to a recruiting station in Wausau, Wisconsin. Diana Gordon is also an active reserve member of the U.S. Army.

23. A search of public profiles on Facebook revealed a profile of Robert Gordon, with photographs of Gordon wearing a U.S. Army uniform and of a desk with a nameplate reading "SSG Gordon," as well as numerous other photographs of Gordon.

24. Kohl's has identified several transactions that tie Robert Gordon to the @OfficialJigLord account and to purchases of items from Kohl's using Kohl's Cash certificates that were originally issued to other persons:

a. On September 13, 2018, Kohl's received online order number 5641130655 via Kohls.com for a Breville Juice Fountain Cold Juicer and a NutriBullet Pro 900-watt blender. The order total was \$279.98. The order was placed on the account of Robert Gordon, 5815 Stella Avenue, Weston, WI, 54476, phone number (254) 630-8732, and email address of mechanical\_dummy@me.com. Kohl's records show that the merchandise was picked up at the Kohl's store located at 3600 Rib Mountain Drive, Wausau, WI 54401. At the time of pickup, payment was made using several Kohl's Cash certificates/coupons issued to four different people: \$20 Kohl's Cash coupon originally earned by M.C. of Massachusetts; \$40 Kohl's Cash coupon originally earned by D.N. of Mississippi; \$50 Kohl's Cash coupon originally earned by P.R. of Florida; \$50 Kohl's Cash coupon originally earned by K.M. of Illinois; Kohl's loyalty certificate originally earned by J.E. of New Jersey. In addition, \$30.30 was charged to a credit card ending in 8166 in the name of Robert Gordon. Kohl's checked the surveillance video associated with this pick-up on September 13, 2018, in the Kohl's store, and pick-up was made by a person in military fatigues who looked identical to other photographs of Robert A. Gordon.

b. On September 14, 2018, the day after the above-referenced purchase, @OfficialJigLord posted on his Twitter account a photograph showing a Breville Juice Fountain and a Nutribullet stacked in the back seat

of a vehicle. The posting associated with the photograph states: "Quick Kohl's cook for the wifey!"

25. Representatives from Kohl's informed law enforcement that certain customers have complained about the loss of their Kohl's Cash, and that Kohl's was able to determine that the customers' Kohl's Cash was used by persons connected to @OfficialJigLord's activities. Kohl's stated that these customers confirmed that they did not authorize anyone to remove Kohl's Cash or loyalty awards from their account, nor did they provide anyone with consent to use their Kohl's Cash or loyalty rewards. Kohl's subsequently took steps to reimburse and/or compensate these customers, resulting in additional losses to Kohl's.

26. The account @OfficialJigLord also appears to have "helpers" who assist @OfficialJigLord in selling the Kohl's Cash and related items. For instance, Kohl's staff found one account, @jighelperDM, which had a title of "Official Jig Helper (Dms open)" followed by the statement: "Here to help to answer all questions that tou [sic] have for @officialjiglrd dms open." Further, Kohl's found a tweet by @OfficialJigLord stating: "you have questions about any jig. DM one of the following: @TryFaceOn @BawbyyJordan @SKRGANG." Kohl's also found another tweet by @OfficialJigLord stating: "If you have questions about jigs. DM one of the helpers below: @TryFaceOn @Potatohead1521 @SKRGANG @BawbyyJordan They will respond to you when they aren't busy. We all have lives to remember that[.]"

27. @OfficialJigLord has been actively engaging in these activities with Kohl's rewards through the present time. For instance, as recently as February 8,

2019, Twitter user “Be Happy” posted a photo of two Kohl’s receipts to @OfficialJigLord. The receipts showed numerous Kohl’s Cash rewards being used for purchases. The post stated “for another success. Always going through with ease. Thank you JL.” This was likely in response to a post on February 6, 2019, in which @OfficialJigLord posted “\$2000 Kohl’s available for Friday’s use. DM if you need.” Then on February 12, 2019, @OfficialJigLord posted “\$111 AMC available (\$40’s and \$50’s) \$150 Kohl’s.”

28. @OfficialJigLord posted on October 5, 2018, that he also had Twitter account @TacticalIntern. On December 4, 2018, Twitter user “Whatsthebiz” tagged @TacticalIntern in a Twitter post that stated, “My boy @TacticalIntern upgraded my life quick fast and in a hurry. Preciate it fam.” There was a photo attached of a Kohl’s receipts on a Sony PS4 box. The receipt showed that multiple Kohl’s Cash rewards were used for the purchase, resulting in savings of \$280.00 and a price of \$21.94.

#### **Information about Twitter**

29. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at <https://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read messages called “Tweets,” and to restrict their “Tweets” to individuals whom they approve. These features are described in more detail below.

30. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

31. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

32. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" to their profile pages.

33. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP

address assigned to the user and the date stamp at the time the user accessed his or her profile.

34. As discussed above, Twitter users can use their Twitter accounts to post "Tweets." Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's own Tweets, as well as a list of all Tweets that include the user's username (*i.e.*, a list of all "mentions" and "replies" for that username).

35. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

36. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location" function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

37. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link. This link service measures how many times a link has been clicked.

38. A Twitter user can “follow” other Twitter users, which means subscribing to those users’ Tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user’s “followers” list) and a list of people whom that user follows (*i.e.*, the user’s “following” list). Twitter users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into “lists” that display on the right side of the user’s home page on Twitter. Twitter also provides users with a list of “Who to Follow,” which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

39. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter’s database.

40. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user’s mobile phone, and the user can also set up a “sleep time” during which Twitter updates will not be sent to the user’s phone.



41. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things.

42. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

43. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

44. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

45. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This "user

attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, communications, “tweets” (status updates) and “tweeted” photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to “tweeted” communications. This geographic and timeline information may tend to either inculcate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner’s state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

46. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

47. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Twitter to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

48. Based on the forgoing, I request that the Court issue the proposed search warrant.

49. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to information associated with the following Twitter profiles:

- @OfficialJigLord at <https://twitter.com/officialjiglord>
- @TacticalIntern at <https://twitter.com/tacticalintern>
- @jighelperDM
- @TryFaceOn at <https://twitter.com/tryfaceon>
- @BawbyJordan at <https://twitter.com/bawbyjordan>
- @SKRGANG at <https://twitter.com/skrgang>
- @Potatohead1521 at <https://twitter.com/potatohead1521>

that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Twitter**

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment A:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;
- d. All IP logs and other documents showing the IP address, date, and time of each login to the account;
- e. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

- f. All "Tweets" and Direct Messages sent, received, "favorited," or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;
- g. All information from the "Connect" tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (*i.e.*, "mentions" or "replies");
- h. All photographs and images in the user gallery for the account;
- i. All location data associated with the account, including all information collected by the "Tweet With Location" service;
- j. All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;
- k. All data and information that has been deleted by the user;
- l. A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user's "following" list and "followers" list);
- m. A list of all users that the account has "unfollowed" or blocked;
- n. All "lists" created by the account;
- o. All information on the "Who to Follow" list for the account;
- p. All privacy and account settings;

- q. All records of Twitter searches performed by the account, including all past searches saved by the account;
- r. All information about connections between the account and third-party websites and applications;
- s. All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. 1343 (wire fraud), § 1029(a)(2) (trafficking in unauthorized access devices), and 18 U.S.C. § 1029(a)(3) (possession of 15 or more unauthorized access devices)) involving Robert Gordon, a/k/a @OfficialJigLord and his accomplices since July 1, 2018, including, for each username identified on Attachment A, information pertaining to the following matters:

- a. Kohl's, including Kohl's merchandise, cash, certificates, coupons, and accounts;
- b. Businesses' customer account information and rewards program information, including usernames, passwords, points, certificates, coupons, codes, and related items;
- c. Selling, purchasing, or advertising of goods or services.



- d. Obtaining, maintaining, transferring, or spending money or other things of value;
- e. Accessing or using personal identifying information, including email addresses, usernames, codes, user IDs, PIN numbers, and passwords.
- f. Unlawful or surreptitious access to information, including information on computers, servers, or websites.
- g. Communications between any of the accounts identified in Attachment A, and communications to or from any of the accounts identified in Attachment A relating to the offense(s), including sales, advertising, customers, potential customers, payments, credit, currency, means of identification, or access devices;
- h. Information relating to preparatory steps taken in furtherance of the offense(s);
- i. Information relating to efforts prevent detection of the offense(s);
- j. Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the offense(s) under investigation and to the Twitter account owner;
- k. Evidence indicating the Twitter account owner's state of mind as it relates to the offense(s) under investigation;

1. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).